STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

April 7, 2005

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to speak about the status of the Federal government's efforts to safeguard our information and systems.

Today I would like to discuss the progress we have made in improving the security of the government's information technology, highlight a few remaining challenges, and identify the steps we are taking to address those challenges. In doing so, I will also address your specific areas of interest.

In March, 2005, OMB issued our second annual report on implementing the Federal Information Security Management Act (FISMA). Much of the information I am discussing today is provided in more detail in our report.

Through our efforts over the past several years overseeing the implementation of FISMA (and its predecessor the Government Information Security Reform Act) we continue to believe FISMA is a sound foundation for improving and maintaining a strong Federal information technology security program – covering both the security of systems and promoting the protection of valuable information.

In short FISMA is working, results are apparent, agencies and Inspectors General are becoming more acclimated to its requirements, and new technical guidelines from the National Institute of Standards and Technology are coming on line to promote further progress. We see no need at this time to revise it in any significant way. In fact, substantial revision could delay additional progress.

Progress in Improving Agency Security Programs

Across the Federal government, through their efforts to implement the requirements of FISMA, most agencies have shown substantial progress in improving their information security programs. Most notably, progress can be shown in increased certification and accreditation of systems, greater annual testing of security controls, more testing of contingency plans, early use of secure system configurations, and improved identification and tracking of security weaknesses.

In our March report to Congress we outlined the progress in the below areas because we believe they are good indicators of the overall health of agencies' security programs. Specifically we reported:

- Certification and accreditation of systems increased to 77% from last year's 62%. In terms of numbers of systems this is an improvement from 4,969 to 6,607 out of a total of over 8,000. Our report highlights the outstanding progress of the Department of Labor (moving from 58% to 96%) and the Department of Transportation (from 33% to 98%).

- Annual testing of system controls increased to 76% percent from last year's 64%. In terms of numbers of systems this is an improvement from 5,143 to 6,515 out of a total of over 8,000.

- Contingency planning increased to 75% from last year's 68% and testing of these plans showed an increase to 57% from last years 48%. The latter is an increase from 3,835 systems to 4,886 out of a total of more than 8,000.

- Finally, in FY 2004, for the first time, agencies reported the degree to which they implemented security configurations for operating systems and software applications. All agencies have begun developing and implementing security configuration policies for at least some of their operating systems.

Securing Agency Critical Infrastructures and Developing Standard Identifications for Federal Employees and Contractors

Related to the goals of FISMA, we are also working with the agencies to improve the identification, prioritization, and security of their critical IT infrastructure. Under the requirements of Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," agencies submitted to OMB plans to protect their critical infrastructure. Working together, OMB and the Department of Homeland Security have evaluated and provided further instructions to the agencies for improvements and next steps.

Additionally, at the President's direction in Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," we have aggressively developed and will soon begin implementing a uniform identification standard for both physical access to Federal facilities and logical access to Federal IT systems.

Our objective is to ensure the identification for government employees and contractors is reliable and can be easily and quickly verified (both visually by a security guard at the front desk and electronically). We know agencies are investing millions of dollars annually in incompatible identification processes and systems, some with questionable value and performance. We also recognize some identifications currently issued by Federal agencies could be forged or stolen thus compromising the government's employees and contractors as well as physical, information, and information technology assets.

Following considerable public notice and comment, including several public meetings, in February 2005 the National Institute of Standards and Technology (NIST) issued the Federal Information Processing Standard (FIPS) 201: "Personal Identity Verification for Federal Employees and Contractors". Agencies will begin implementing the standard in October of this year.

Continuing Challenges

While progress has been made, deficiencies in agency security procedures and practice remain, much of it due to inconsistent implementation within agencies and across the government. Continuing weaknesses reflect the complexity of securing the Federal government's vast number of information systems. Examples of common deficiencies noted by agency Inspectors General (IGs) include:

- <u>Agency-wide Plans of Action and Milestones (POA&Ms).</u> OMB asked agency IGs to assess, against specific criteria, the quality of the agency-wide POA&M process. OMB policy requires agencies to prepare POA&Ms for all programs and systems where an IT security weakness has been found. Although 18 IGs have verified their agency's management of an effective POA&M process, six IGs revealed overall deficiencies in their agency's process.

- <u>Quality of certification and accreditation process</u>. This year for the first time, IGs were asked to assess the overall quality of their agency's certification and accreditation process, including the degree to which agencies follow NIST guidance. Six IGs rated the agency certification and accreditation process as "good", and nine rated it as "satisfactory;" however, seven IGs rated the process as "poor" and two were not able to complete the evaluation. None of the IGs rated the certification and accreditation process as failing.

In addition to deficiencies noted by the agency IGs, we have identified other areas of concern through our own reviews and in consultation with other experts including the agencies and the Government Accountability Office (GAO). Some of these areas are new while others continue from prior years. They include:

- Overall inconsistency in agency and government-wide FISMA implementation and self-evaluations and IG evaluations
- Potentially unnecessary duplication of effort and resources across government
- Ensuring adequate security of contractor provided services
- Transition to Internet Protocol Version 6

While we believe FISMA itself and implementing guidance from OMB, NIST, and national security authorities is sufficiently comprehensive and detailed to address these concerns at a policy level, consistent implementation is difficult and requires considerable expertise and resources from each agency (including small and independent agencies).

Below, I will address some specific plans to address the above challenges, but first I want to begin by answering directly one of the questions asked in your invitation letter, i.e., whether there is a need for an IG auditing framework similar to that used in financial audits?

We have found the IG's analysis extremely valuable in gaining additional insight into agency IT security programs and operations. Much of the analysis in our annual report, and we know your annual security report card, comes from the IG's findings. We have been able to use this information to validate agency reports and better hold agencies accountable in various ways including through the President's Management Agenda Scorecard process.

At the same time, like the agencies themselves (including CIOs and operational program officials), across the IG community IGs have varying capacities including available resources to conduct comprehensive reviews, different levels of security expertise, and across the IG community differing methodologies and perspectives on what comprises a sound security program and what constitutes proper implementation of FISMA and OMB policies. As a result, we have found relying solely on an IG's assessment is not always adequate.

Therefore, to the extent an IG evaluation framework would promote greater consistency we would support it. However, we do note the concerns below.

First and foremost, we strongly believe the work of the IGs should to the maximum extent practicable, be integrated into and not separated from agency IT security programs. This is especially important to avoid agencies' and IGs competing for scarce security expertise—taking away essential resources needed to implement and maintain security programs and shifting them to IG specific evaluations. We have already seen examples of this shift in several agencies and are troubled by it. It does not in our view promote sound security programs. We have stressed the importance of interaction in our FISMA implementing guidance. Again, the IGs and the agencies should work together throughout the year, share resources to the maximum extent practicable, and improve the overall program, not simply produce better evaluation reports. Furthermore, IGs and agencies should also share findings from program and system reviews as they become available. OMB encourages IGs to deliver interim reports to agency officials in instances where potential significant deficiencies have been identified. Timely sharing and awareness of security weaknesses and significant deficiencies helps prevent further loss and damage to the agency's overall performance.

Second, we are concerned with adopting strict and specific review requirements for FISMA purposes if they would in any way limit the essential interaction described above. We are particularly concerned with requiring IGs to perform an "audit" as opposed to FISMA's "evaluation." By requiring an evaluation but not an audit, FISMA intended to provide IGs flexibility as to the degree of cooperation with CIOs and program officials. OMB encourages IGs to take advantage of this flexibility while ensuring the appropriate degree of accuracy, independence, and objectivity. Moreover, unless any review requirements were very closely aligned with OMB's implementing policies and NIST guidance, agencies could be evaluated by IGs against one set of criteria and by OMB against another different set. We see this today when IT security programs are evaluated by IGs using the Federal Information Systems Control Audit Manual (FISCAM). While FISCAM's underlying principles are essentially the same as OMB's security policies, there are sufficient differences in the specific details as to make easy correlation unnecessarily complex, time-consuming and in some cases unhelpful.

Throughout the past several years, we have had ongoing discussions with key members of the IG groups to solicit feedback on the FISMA reporting and evaluation process. In particular this year, we have engaged the President's Council on Integrity and Efficiency and we have discussed ways to make their evaluations more consistent.

Also to promote increased consistency in oversight and reporting, we have asked the IGs to participate in OMB's newly formed IT Security Line of Business which I discuss in greater detail below. We expect this line of business will not only lead to a *de facto* IG and CIO reporting framework, but, more importantly a stronger Federal government-wide IT security program.

Activities to Improve IT Security Performance

IT Security Line of Business

On March 23, 2005, OMB kicked off an information systems security line of business co-managed by the Department of Homeland Security and the National Security Agency. Since the kick-off, an interagency task force has formed and met twice. The task force comprises representatives from all 24 CFO Act agencies, the Small Agency Council, the IG community, and NIST.

In just two weeks the task force has come to consensus on its vision and goals. On Monday, April 4 it released a public request for information soliciting IT security best practices from industry and government.

The vision of the line of business task force is:

> *"The Federal Government's information systems security program enables agencies' mission objectives through a comprehensive and consistently implemented set of risk-based, cost-effective controls and measures that adequately protects information contained in Federal Government information systems."*

To achieve the vision, the task force has set the following goals:

- Identify problems and propose solutions to strengthen the ability of all agencies to identify and manage information security risks,
- Develop improved, consistent, and measurable information security processes and controls across government, and,
- Achieve savings or cost-avoidance through reduced duplication and economies of scale.

In order to achieve the vision and work towards the goals, the task force has identified five activity areas for consideration in the development of common IT security solutions. These five areas closely map to FISMA and include: training; threat awareness and incident response; program management; security in the systems lifecycle development process; and selection, evaluation, and implementation of security products.

Over the next few months, task force members will be gathering and analyzing information in these areas to develop recommendations for each of the five areas which could most benefit from a common solution, collaboration, or standardization of processes. Consolidated business cases will then be developed to implement any common solutions and inform the agencies' FY 2007 budget requests and OMB's decisions.

President's Management Agenda Scorecard

While the task force performs its work, OMB will continue to use our existing oversight mechanisms to improve agency and government-wide IT security performance. Specifically, as I have described to the Committee in the past, we are using the President's Management Agenda Scorecard and quarterly reporting process to drive agency progress.

By including IT security in the PMA Scorecard, we underscore while it clearly has a technical component, it is at its core an essential management function. Therefore, we have greatly increased executive-level attention and accountability.

As you know, the PMA was launched in August 2001 as a strategy for improving the performance of the Federal government. The PMA includes five government-wide initiatives, including Expanded Electronic Government (E-Government). The goals of the E-Government initiative are to ensure the Federal government's annual investment in information technology significantly improves the government's ability to serve citizens and to ensure systems are secure, delivered on time and on budget.

Each quarter, agencies provide updates to OMB on their efforts to meet government-wide goals. The updates are used to rate agency progress and status as either red (agency has any one of a number of serious flaws), yellow (agency has achieved intermediate levels of performance in all the criteria), or green (agency meets all the standards for success).

Information technology security is one of a number of critical components agencies must implement to get to green (or yellow) for the E-Government scorecard. If the security criteria are not successfully met, agencies cannot move forward, regardless of their performance against other E-Government criteria. Agencies are publicly accountable for meeting the government-wide goals, and scores are posted quarterly at http://results.gov/agenda/scorecard.html

To "get to green" under the Expanding E-Government Scorecard, agencies must meet the following three security criteria:

- Demonstrate consistent progress in remediation of security weaknesses
- Attain certification and accreditation of ninety percent of their operational systems, and,
- Maintain an IG assessed and verified agency POA&M process.

In order to "maintain green," by July 1, 2005, agencies must have:

- Certified and accredited all systems,
- Installed and maintained all systems in accordance with security configurations, and,
- Consolidated and/or optimized all agency infrastructure to include providing for continuity of operations.

Integrating IT Security into the Budget Process

OMB policy requires agencies to submit a Capital Asset Plan and Business Case justification for all major information technology investments. In their justification, agencies must answer a series of security questions and describe how the investment meets the requirements of the FISMA, OMB policy, and NIST guidelines. The justifications are then assessed against specific criteria including whether the system's security, planned or in place, is appropriate.

Transition to Internet Protocol Version 6 (IPv6)

Late last fall, OMB directed the agencies to provide a preliminary report on their planning activities for the transition to IPv6 from the current IPv4. Only the Department of Defense has undertaken any significant activity in this area.

Since that time, the Department of Commerce and the Government Accountability Office have produced draft reports on the complexity and risks associated with this transition. While I am not prepared to nor should I discuss the details of these draft reports, I can say OMB is sufficiently concerned the complexities of the transition require special action. Therefore, we will begin, through the CIO Council, developing a comprehensive transition planning guide. We have yet to finalize the details for this activity, but will begin this effort soon.

Conclusion

Over the past year, agencies made significant progress in closing the Federal government's information technology security performance gaps. I would like to acknowledge the significant work of agencies and IGs in conducting the annual reviews and evaluations. This effort gives OMB and Congress much greater insight into agency IT security status and progress.

However, uneven implementation of security measures across the Federal government leaves vulnerabilities to be corrected. I have described the ways OMB will use existing management and budget processes and the new line of business to promote greater compliance with law, policy, and guidance and thereby improve agency-specific and the government-wide security program.

While notable progress in resolving IT security weaknesses has been made, problems continue and new threats and vulnerabilities continue to materialize. Much work remains to improve the security of the information and systems that support the Federal government's missions. To address these challenges, OMB will continue to work with agencies, GAO, and Congress to promote appropriate risk-based and cost-effective IT security programs, policies, and procedures to adequately secure our operations and assets.

But again, we believe FISMA is more than adequate in its current form to support all needed improvement efforts.